DOCUMENT RESUME

ED 141 818 CS 203 517

AUTHOR O'Reilly, James T.
TITLE The Privacy Act of 1974.
INSTITUTION Freedom of Information Center, Columbia, Mo.
REPORT NO FOI-342
PUB DATE Sep 75
NOTE 7p.

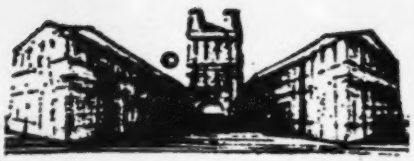
EDRS PRICE MF-$0.83 HC-$1.67 Plus Postage.
DESCRIPTORS *Censorship; *Civil Liberties; *Constitutional Law; *Freedom of Speech; Government Role; *Information Dissemination; Information Utilization; Laws
IDENTIFIERS *Freedom of Information; *Privacy Act of 1974

ABSTRACT

This report describes the possible impact of the comprehensive Privacy Act of 1974, which went into effect on 27 September 1975. Specifically, the implications of the act for limitation of disclosure, federal information collection, individual access, private suits; criminal provisions; and exceptions to the provisions of the law are detailed. In addition, the formation of the Commission on Privacy is described, and possible administrative problems are outlined. Special attention is given to the role of the press in regard to the act and to the relationship between the Freedom of Information Act and the new provisions for privacy. It is concluded that the act, as it becomes an effective part of the information-gathering process, will provide the public with a major check upon the government's functions as collector, digestor, and disseminator of citizens' personal data. (KS)

****
* Documents acquired by ERIC include many informal unpublished *
* materials not available from other sources. ERIC makes every effort *
* to obtain the best copy available. Nevertheless, items of marginal *
* reproducibility are often encountered and this affects the quality *
* of the microfiche and hardcopy reproductions ERIC makes available *
* via the ERIC Document Reproduction Service (EDRS). EDRS is not *
* responsible for the quality of the original document. Reproductions *
* supplied by EDRS are the best that can be made from the original. *
****

ED141818



SCHOOL OF JOURNALISM, UNIVERSITY OF MISSOURI AT COLUMBIA
SEPTEMBER 1975

U S DEPARTMENT OF HEALTH, EDUCATION & WELFARE
NATIONAL INSTITUTE OF EDUCATION

THIS DOCUMENT HAS BEEN REPRODUCED EXACTLY AS RECEIVED FROM THE PERSON OR ORGANIZATION ORIGINATING IT. POINTS OF VIEW OR OPINIONS STATED DO NOT NECESSARILY REPRESENT OFFICIAL NATIONAL INSTITUTE OF EDUCATION POSITION OR POLICY

FREEDOM OF INFORMATION CENTER REPORT NO. 342

THE PRIVACY ACT OF 1974

This report was written by James T. O'Reilly, an Ohio attorney.

Discussion of the protection of individual privacy from federal intrusion is likely to evoke images of White House "enemies lists," of constitutional struggles between civil liberties and government prerogatives and, ultimately, of Orwell's 1984, a chilling vision of electronic monitoring of even the most intimate act. After long years of debate, a comprehensive federal privacy law passed the Congress in 1974 as a solid legislative decision in favor of individual privacy and the "right to be left alone."

When that new statute goes into effect on September 27, 1975, it is expected to have a major impact on information collection by the federal government, on the privacy of personal information of those subject to federal studies and upon those in the news media who rely on the government as a primary source for information.

The Privacy Act of 1974 was debated and passed by the Senate on November 21, 1974, the same day that body voted to override President Ford's veto of the amendments to the Freedom of Information Act. The complex Privacy Act is replete with provisos, exceptions and exemptions; this report will attempt to explain its nine key provisions, to suggest the impact of the press on its adoption and, in turn, its effect on the working press, and to identify the areas of its complementary and conflicting interaction with the Freedom of Information Act.

The Privacy Act is complex because it undertakes to reach all federal information-gathering and information-disclosure operations. That task alone is formidable. Congressional inquiry of federal agencies revealed that no cataloguing of all the various information systems had been made. A 1971-73 study by the Senate subcommittee on constitutional rights, the best estimate to date, found 858 federal data banks with 1,246,000,000 files on individuals.[1] Moreover, as S.3418, the privacy bill sponsored by Sen. Sam Ervin (D-N.C.), took shape from the many privacy proposals that sought to remedy the abuses of federal information systems, the statute grew in length, scope and complexity.

In its final form, the act contains nine key provisions:

—limitation on disclosures of individually identifiable information by federal agencies;
—limitation on the means and purposes of federal data collection from individuals;
—published notice of the existence and scope of federal data banks holding individually-identifiable information;
—an individual's right of access to his own file;
—an individual's right to correct errors in file information or to insert in the file a formal statement dissenting from its accuracy;
—establishment of new legal rights to sue the agencies for access to a file, for its correction or for damages incurred as a result of incorrect data in the file;
—general application of the act to all files, with very narrow exempt classifications;
—criminal penalties for misuse or unauthorized disclosure of personal information from files and for maintaining secret data systems; and
—establishment of a federal Privacy Protection Study Commission.

The Privacy Act applies to federal information about activities of private citizens and actions taken against private citizens, as well as to identifying information and personal data about individuals. It does not cover partnership or corporation files, although files of individual employee's actions are apparently subject to the act. In general, no personal information may be disclosed by the file keeper except in rigidly defined situations. The four principal exceptions on nondisclosure under the act are: disclosures made in the course of agency activities, on a "need-to-know" basis; disclosures pursuant to an FoI Act request; disclosures for valid law enforcement purposes, made under a strictly controlled request procedure; and disclosures made to the individual subject of the file.

Limitations on Disclosure

In keeping with its "no disclosure unless authorized" rationale, the act emphasizes the need for "informed consent" of the individual, both when the information is collected and when it is released. Transfers of data from a collecting agency to another federal agency are strictly controlled. While the drafters intended that commonplace disclosures would continue — for example, inquiries and responses about a person's status as a federal licensee — the act limits release of the licensee's personal information submitted to obtain the license.

Security against "leaks" is provided both by criminal penalties and by a requirement that agencies affirmatively remind employees of their own "ethical obligation" to protect the confidential status of files. Methods must be adopted to minimize or eliminate the potential of file data to cause "substantial harm, embarrassment, inconvenience,

Summary: The comprehensive Privacy Act of 1974, which goes into effect on Sept. 27, 1975, will have a major impact on the federal government's collection, use and dissemination of information on individual citizens.

Additional copies 50¢ each

CS 203 517

or unfairness" to the subjects of the file. The act, which contains innovative provisions for private suits against federal agencies for misuses of information, also provides for an "audit trail," by which a person may track down those who have seen the contents of his personal file. He may, then, from that search discover the results of the existence of incorrect data.

Federal Information Collection

The extensive hearings on privacy legislation raised serious questions about the propriety of many federal demands for personal information. Abuses of the collection process caused the Congress to adopt extreme limitations on information-gathering, and at least one official has predicted that fewer records will be kept by the federal government.[2] Information-gathering from individuals will be permitted only if an official at the "highest level" of an agency has made a determination that collection is necessary to carry out a duty imposed by statute or executive order, and that other means would not be sufficient to meet the needs of the program.

All requests for personal information must be clearly marked as "voluntary" or "mandatory," must state the legal authority for collection, must reveal the uses and purposes to which the agency will put the information and must advise the individual of any adverse action which would result from failure to respond. No files may be kept of an individual's exercise of First Amendment rights unless they are expressly authorized by Congress or are "pertinent to and within the scope of an authorized law enforcement activity." A description of each data system containing personal information, and its legal authorization, must be published by each federal agency along with procedures by which individuals can obtain copies of their files. And, in light of the use which may be made of the information once disclosed, all information gathered must be kept with the accuracy, relevance, timeliness and completeness needed to assure fair treatment of the subject of the file.

A single federal publication will list all agency data banks which contain individually-identifiable information, and failure of any agency — including the CIA and FBI — to disclose the existence of a data system can be punished by a $5,000 fine. Advance notice must also be given of new file systems, so that individuals who are or may be included will know how to gain access to the new files. A list of FBI files might include, for example, all persons who have subscribed to specific foreign newspapers; a subscriber may then write to the agency and obtain access, with some limited exceptions, to his file. Both the Senate and House bills were insistent that all agencies list the existence of all personal files, regardless of the exemptions which might apply to contents of individual files.[3] Congress intended both that individuals know the scope of data gathering and that Congress have the opportunity to challenge information collection programs on budgetary or statutory-authorization grounds.

Individual Access

To many people, the act's most important feature is the guarantee of individual access. Each citizen has the right to know of the existence of the systems, the existence of an individual file and (with exceptions) the contents of the file affecting or relating to that person. Deletions from the file may be made for the names of informants, however, after the effective date of the act only the names of those expressly promised confidentiality can be deleted when files are assembled for release. Releasable information must be provided in legible format such as copy or computer printout.

When an individual receives access to his own file, the agency must disclose the uses and the prior recipients of that file, to permit the subject to "trace and correct the further uses of any inaccurate information, or to take any necessary action to retrieve it from improper disclosure."[4] The nature and names of sources, except where exempt, must also be disclosed. If file information is incorrect and tracing of uses reveals that such misinformation has resulted in a disadvantage — denial of a government loan, for example — the the agency can be sued for damages. The "paper maze" can be explored in person by the individual, or by mail upon written request; in both instances the agency must demand positive identification from the requester to prevent improper release of information to an impostor.

When an individual discovers that any file information is incorrect he is authorized by the act to make the necessary corrections. Through special corrections procedures, the individual may request amendment of his files. The agency at fault must acknowledge receipt of such request within ten days and must "promptly" thereafter decide whether to correct the records. If the agency insists that the file is correct, it must give the individual a statement of reasons, an explanation of the agency appeal process and the name of the person to whom to address the appeal for corrections. Upon receipt of appeal, the agency must decide within 30 days to correct or give the individual notice of his right to sue for correction. In addition, the agency must accept for filing an individual's statement of disagreement or "concise" statement of explanation of the file information. Such statements will be made part of the file and must accompany all succeeding releases of that file. Though the provisions for administrative appeal and court action regarding access and correction resemble the FoI Act provisions, the absence of a fixed deadline for agency response may well mean that Privacy Act requesters will be subjected to longer delays than are permitted by the statutory maximums of the FoI Act.

Private Suits

For many years, citizens were essentially powerless in defending themselves against government invasions of privacy. No such doctrine as sovereign immunity protected their interests. In 1896, however, Supreme Court Justice Louis Brandeis, in an article which was the genesis of modern legal thought on privacy rights, proposed stronger remedies for those whose privacy is invaded by government:

> It would doubtless be desireable that the privacy of the individual should receive the added protection of the criminal law, but for this, legislation would be required. . . . The common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands. Should the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiousity? [5]

The drafters of the Privacy Act attempted to correct such legislative deficiencies by providing liberalized remedies for individuals against the state.[6] Three types of litigation are provided for in the act. An individual may, through court

litigations, sue for access to the file or for its amendment or correction. A person affected may also sue for damages when an agency fails to comply with the act so as to injure the person or "fails to maintain any record concerning the individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness. . . ." Successful litigants in such damages actions will receive a minimum of $1,000 plus costs and attorneys' fees.

Two different proposals were deleted. The administration successfully fought a proposal in the Senate bill that permitted damages to run against the individual employee of the agency.[7] A minority House report which called for punitive damages to be permitted as an additional award when abuses were discovered and proven was also left out of the final bill. [8]

Although the terms of this remedial section are attractive enough to make it likely that much litigation will develop in the early years of the act's existence, it should be noted that the test to be applied is a strict one. Plaintiffs must prove that they were the subjects of a record; that the agency failed to use a full measure of fairness in assuring the record's relevance, accuracy, timeliness or completeness; that a decision had been made on the basis of the record affecting the individual's rights, character, opportunities or benefits; and that an adverse determination was made based upon the improperly handled record. With this difficult burden of proof, it is probable that many more cases will be filed than won.

Criminal Provisions

Even with a $1,000 minimum recovery on civil suits, limitations of resources will necessarily restrict people in the exercise of their right to sue. As the Senate report noted, "private enforcement through litigation is not likely to affect more than glaring violations of the Act. Much will depend on the zeal and the good faith of the Attorney General and the President in enforcing the terms of the new law." [9]

The prosecutorial "zeal" called for by the Senate would affect many sources of "leaks" of personal information with criminal misdemeanor penalties, including a $5,000 fine. For all offenses under the act, both intent and knowledge of illegal activity are required as elements of the government's proof. The primary prohibition is that against disclosure of personal information covered by the act to **any person or** agency not entitled to receive it. The "agency" language strengthens the prohibitions against unregulated transfers of information within federal agencies, such as from a licensing agency to a law enforcement unit. Any transfers permitted before the act's effective date must be carefully documented and authorized after September 27, 1975. Employees who ignore the act may be criminally liable.

A second criminal provision imposes liability on those who maintain secret files — a data bank concealed from the public by withholding its existence from the annual **Federal Register** publication, for example. This reflects the absolute congressional mandate that existence and identification of all data banks be a matter of public record.

The final criminal provision authorizes prosecution of anyone who obtains or attempts to obtain a personal record from an agency under false pretenses. This would cover both an outsider's attempt to use the access provisions to obtain another person's file, and an agency employee's falsification of authority to examine personal information.

Exceptions to the Provisions of the Law

The act's broad provisions have several narrow exceptions, which Congress applied to those areas where a genuine concern existed that some personal information not be released to file subjects. National security files maintained by the CIA were felt to deserve a general exemption from disclosure, as were the files of active criminal cases of criminal law enforcement agencies. Specific exemptions may be claimed for files within other national security agencies and for other law enforcement purposes, but these exemptions must be first justified by a published set of reasons in the **Federal Register**.

Sen. Sam Ervin divided the "narrow exceptions" to limit national security exemptions into two classifications: national defense posture and matters concerning "sensitive dealings with foreign countries." [10] He also stated during the Senate debate that the head of an agency engaged in criminal law enforcement could invoke an exemption if he found that the dissemination provisions of the act "would impede the accomplishment of his department's professional duties or statutory duties." In response to a question, Sen. Ervin specifically limited the intended coverage of the exemptions to agencies which have a national security or criminal law enforcement mission, and he excluded agencies like Commerce or Agriculture Departments, some of whose functions could affect the national security or foreign policy. [11]

In keeping with the congressional fear that secret information has caused unrecognized harm to individuals, the exemptions were themselves subject to an exemption. If any requester can show the agency or a court that maintenance of the information may affect his eligibility for any "right, privilege, or benefit," the record must be disclosed; only the names of informants may be deleted. And the availability of criminal agency exemptions from disclosure may be short-lived, for Congress and the Justice Department are separately working on another privacy statute to supplement the Privacy Act in the area of law enforcement records. [12]

The Commission on Privacy

The Privacy Act also establishes a seven-member advisory commission to study many of the incomplete privacy proposals raised in the development of the act. With a relatively small budget of $1,500,000, the commission is charged with a broad variety of inquiries and with the drafting of legislation to correct oversights in the act itself. Among the topics for study are: private data bank access and maintenance regulations; local and regional government data bank standards like those in the act; collection, storage and use of personal information in banking, insurance, education and "telecommunications media" data systems; mailing list regulation; and a proposal that the Internal Revenue Service be prohibited from transferring personal information to other agencies or to state authorities. Many objections of the Ford Administration to some privacy proposals were accommodated by deleting objectionable sections and referring those issues for further study by the commission.[13]

Administrative Problems

The Privacy Act requires each agency to publish a complete list of all records systems which contain individually identifiable information, and to establish rules regulating maintenance, collection and access to those files. In the annual **Federal Register** collection of Privacy Act publications, each agency's rules on access, appeals and

exemptions must be published at the same time that the agency lists the name of each data system, its routine uses, categories of persons listed, information sources used and other information about the system. The first publication is scheduled for September 27, 1975, but there are indications that the deadline may not be met. A request by the Office of Management and Budget to move the deadline back to March, 1976 was approved by the Senate but not finally adopted. [14] Ironically, OMB's own deadlines for agency preparation of Privacy Act information have already been missed by more than half the federal agencies. [15]

When a request for access is received, the agency is required (unless exempted) to state whether a file exists and, if it does, to make the file available in a legible form to the individual. A file may be requested in person or by mail, and only a reasonable copying charge may be required. The agency is required by the act to take precautions to make positive identification of the requester as the subject of the file. Each request is governed by agency rules and by the act's exceptions; it is predictable that criminal file requests will be the first cases to be litigated under the act.

Handling Privacy Act requests will be a burdensome chore for the agencies. Agencies will receive a wide variety of requests from a wide variety of requesters, and ironically they cannot even demand the Social Security number of a requester as a condition of identifying the file subject, because another section of the Privacy Act restricts that number's use as an identifier.

The workload on agencies such as the FBI and Justice Department can be expected to exceed the flood of requests which accompanied the FoI Act amendments in early 1975. During that period, much of the Justice Department's attention was devoted to FoI requests to the detriment of other activities — and the Privacy Act requests will be even more work for the same budgetary resources.

Costs of the Privacy Act legislation will be high during the first of two fiscal years, as publication requirements, computer time and processing of requests cause enormous demands on administrative time and energies. No cost estimate was made while the act was still being developed; indeed, the OMB advised the Senate that such a cost estimate was impossible.[16] In lieu of a cost estimate, the Senate report quoted from a report on privacy protection activities prepared for the Department of Health, Education and Welfare:

> We believe that the cost to most organizations of changing their customary practices in order to assure adherence to our recommended safeguards will be higher in management attention and psychic energy than in dollars. These costs can be regarded in part as deferred costs that should already have been incurred to protect personal privacy, and in part as insurance against future problems that may result from adverse effects of automated personal data systems. [17]

The absence of any legislative estimate of costs makes it probable that no real estimate will be available for 18-24 months from the December 31, 1974 date of enactment.

Press Involvement With the Act

The loss caused by the Privacy Act of "inside" sources of information is a serious concern of the press. During development of the legislation, groups such as the American Society of Newspaper Editors raised three issues which are dealt with in the final statute: a concern that reporters' contacts with agencies be less strictly regulated than other contacts; a fear that the beneficial aspects of "whistle-blowing" against misconduct in office may be lost under criminal penalties; and a desire to preserve uses of the FoI Act in achieving access.

"Nonregular access" recording was the first press concern. Instead of a file-by-file history of information recipients, which would have been burdensome and would have immediately identified press contacts by person, date and reason, the act creates instead an "audit trail" — a classification of regular users which can include members of the press along with agency employees and which does not require specific recording. The agency retains discretion to make the press "nonregular" and thus to require file-by-file recording of access, but it is hoped by the changed classifications that press access will be usually considered "regular."

The Senate report viewed "whistle-blowing" as a virtue, especially in areas of official misconduct, since it contributes to "disclosure of wrong-doing to Congress and the press which helps to promote 'open government'." [18] The Senate responded to this by deleting the sanctions against such disclosure provided by section (i)(1); but this provision was later reinserted and appears in the act, although the statutory standard for conviction is specific and may be difficult to prove. [19] On the other hand, the penalties structure is similar to the criminal sanctions applied to disclosure of information about trade secrets, tax information, etc. If the person can be found who leaked information to the press about an employee's past history or a licensee's statement of personal income, criminal prosecution could result.

The third press concern which affected the act's development was its interrelationship with the FoI Act. Conditions on the disclosure of information, such as reporting of contacts and pledges of confidentiality in handling, were deleted by Congress in response to these concerns. The Senate Committee found it unreasonable and "contrary to the spirit" of the FoI Act to impose such conditions on FoI disclosure:

> While the Committee intends in this legislation to implement the guarantees of individual privacy, it also intends to make available to the press and public all possible information concerning the operations of the Federal Government in order to prevent secret data banks and unauthorized investigative programs on Americans. [20]

The Act's Impact on the Press

The methods of Washington journalists will not be greatly changed by the Privacy Act, though the availability of background data on individuals from "sources close to" or "sources within the" agencies may be lessened by the criminal and administrative provisions of the act. If agencies choose to use specific recording of press contacts rather than the more vague "audit trail" classifications of "routine" access, there will be a means for tracing "leaks." And the past practice of information collection through telephoned pseudonyms may cease when reporters learn that even the attempt to get information under false pretenses carries a $5,000 fine.

An obvious benefit of the act for the press is the required publication of each and every federal records system. If a federal agency has a computerized data bank on college demonstration participants or of contributors to radical causes, the identity, uses and authorization for the system

will become public knowledge. According to the Senate report, the press will contribute to Privacy Act enforcement "through its investigation and exposure of wrongdoing, a function eased by the requirements . . . that decisions be made on the open record by responsible officials and that precise notices be published containing the details of government policy where it affects personal privacy." [21]

The Privacy Act may be predicted to provide much newsworthy material for journalists. Apart from the more sensational incidents such as the attack by Rep. Bella Abzug (D-N.Y.) on the CIA for maintaining a file on her attorney-client transactions, the press will undoubtedly find long-term interest in two types of lawsuits arising from the act. Damages actions will be brought against agencies by persons who belatedly discover that errors in federal data caused them to be denied jobs, loans or other privileges. For the first time, there may be large judgments against federal agencies for losses incurred because of dissemination of erroneous or detrimental file information from agency to agency. The second type of privacy suit will concern correction of disputed file statements; agencies which insist that a file item is correct should anticipate being sued and should also expect an additional challenge in many cases to the agency's authority for collecting the information.

Reporters covering Congress can expect a flurry of bills to revoke agency authority to collect certain types of information on citizens, once the whole scope of federal data-collection becomes known. One purpose of the **Federal Register** listing, according to the congressional reports on the act, is to alert Congress to systems which Congress may have overlooked and may want to eliminate for budgetary or substantive reasons.

The Privacy Act and the FoI Act

It was appropriate that the FoI Act amendments and the Privacy Act should have been debated and passed by the Senate on the same day, November 21, 1974. The FoI Act and the newer Privacy Act are complementary in their advocacy of more open government, but they differ in two important respects.

The FoI Act mandates disclosure, with narrow exceptions covering trade secrets, national security information, criminal law enforcement files and files which would if disclosed constitute "unwarranted invasions of personal privacy." By contrast, the Privacy Act mandates non-disclosure of individually identifiable information and is concerned with informed consent of the file subject prior to any government dissemination of the information. As a second distinction, the Privacy Act imposes an affirmative responsibility on each agency to adopt rules and regulations, while the FoI Act responsibilities rest on a case-by-case determination by each federal agency. Writing in **National Journal Reports**, journalist Richard E. Cohen assessed the quandary posed by these two statutes:

> While the goal of each law is similar — more responsible collection and use of federal records — the means of attaining the goals are sufficiently different that some federal officials contend they may face an Orwellian dilemma of violating one law if they release a record and violating the other law if they do not release the same record. [22]

On careful review, this problem is of less concern than it appears at first glance. The FoI Act permits an agency discretionary authority to disclose or to refuse disclosure of "personnel and medical and similar files, the disclosure of which would constitute a clearly unwarranted invasion of privacy." [23] The freedom of the agency to decide to release rather than to claim the exemption has been upheld by several recent court cases. Thus, a submitter of information has no real authority to prevent its dissemination if an agency decides not to claim the right to exempt that information from disclosure. A Privacy Act refusal to disclose, then, or an authorized disclosure in accordance with that act, will generally not result in any liability under the FoI Act. The House version of the Privacy Act proposed to limit routine disclosures to those "which would not violate the spirit of the Freedom of Information Act by constituting a 'clearly unwarranted invasion of personal privacy'," but this was not adopted. [24]

Section (q) of the Privacy Act specifically prevents the use of FoI Act exemptions to deny individuals access to their own files. It is reasonable to predict that, wherever disclosure to the file subject is concerned, the FoI Act will be no bar to disclosure; but the requests from outsiders for FoI release of personal information will be much more likely to meet denials.

Uncertainty about release will become a problem in delays at the agency level. Unlike the provision for responses within specified time limits to FoI requests — ten days for initial response and 20 days for appeals — the response to a Privacy Act request need meet no time deadline. Even when the agency is sued for access under the Privacy Act's suit provisions, the courts are not required to give special treatment to the litigation, as they are required to "expedite" the FoI suits. Delay will be inevitable under the terms of the Privacy Act — if agencies choose to approach it as an administrative headache rather than as a beneficial aspect of "openness" in government.

Conclusion

On September 27, 1975, the business of government information-gathering will reach a milestone as a result of a deliberate congressional choice in favor of individual privacy. Secret intelligence operations like the "White House Plumbers" became the catalyst for long-gestating proposals toward a comprehensive privacy protection statute. As the act becomes an effective part of the information-gathering process, it will provide a major check for members of the public upon the performance of government's function as a collector, digestor and disseminator of personal data on citizens.

During debate on the act, Sen. Edmund Muskie, (D-Me.) quoted former HEW Secretary Elliot Richardson: "Government is not the owner of information on individuals, but only the trustee." [25] As the press and the public monitor its performance, government may begin to treat public files as a public trust.

FOOTNOTES

1. Richard E. Cohen, "Agencies prepare regulations for implementing new privacy law," **National Journal Reports**, May 24, 1975, p. 775.
2. **Ibid.**, p. 774.
3. The Senate version, S. 3418, was passed and adopted. For provisions of H. R. 16373, see H. R. Rep. No. 1416, 93d Cong., 2d sess. (1974).
4. S. Rep. 1183, 93d Cong., 2d sess. (1974). Reprinted in **U. S. Code Congressional and Administrative News**, p. 6975.
5. Samuel Warren and Louis Brandeis, "The Right to Privacy," **Harvard Law Review** IV (1896), 193.
6. H. R. Rep. 1416, 93d Cong., 2d sess. (1974), pp. 9-10.
7. 120 Cong. Rec. 19832 (Nov. 21, 1974).
8. H. R. Rep. 1416, **op. cit.**, p. 38.
9. S. Rep. 1183, **op. cit.**, p. 6943.

10. 120 Cong. Rec. 19852 (Nov. 21, 1974).
11. **Ibid.**, in response to a question from Sen. Bayh.
12. Cohen, **op. cit.**, p. 777.
13. 120 Cong. rec., 19831-33 (Nov. 21, 1974). Senate discussion of these objections.
14. **Ibid.**, 19832.
15. Five weeks after the OMB deadlines, only 50 of the nearly 100 agencies had submitted their compliance plans. (Cohen, **op. cit.**, 777)
16. S. Rep. 1183, **op. cit.**, 6959
17. **Ibid.**
18. Ibid., 6942.
19. Ibid., 6995.
20. Ibid., 6985.
21. Ibid., 6943.
22. Richard E. Cohen, "New information laws gets heavy use from public, businesses," National Journal Reports, July 5, 1974, p. 985.
23. 5 U.S.C. 552 (b) (6).
24. H. R. Rep. 1416, **op. cit.**, 13.
25. 120 Cong. Rec., 19838 (Nov. 21, 1974).